Threat Intelligence

Traccia 1

Il sistema di valutazione di ThreatConnect è basato su due principali livelli di valutazione: il Threat Rating e il Confidence Rating. Ecco una descrizione dettagliata di ciascun livello e delle sue caratteristiche:

Threat Rating (Valutazione della Minaccia)

Il Threat Rating misura quanto una minaccia rappresentata da un indicatore (Indicator) è pericolosa, utilizzando una scala da 0 a 5 teschi:

1. **Unknown (0 teschi)**
   - **Descrizione:** Non ci sono sufficienti informazioni per valutare il livello di minaccia.
   - **Esempio:** Indicatori ancora in fase di revisione senza dati definitivi.
2. **Suspicious (1 teschio)**
   - **Descrizione:** Attività sospetta osservata, ma nessuna attività dannosa confermata.
   - **Esempio:** Attività anomala su un URL senza prove di danno.
3. **Low Threat (2 teschi)**
   - **Descrizione:** Indica un avversario non sofisticato, probabilmente opportunistico e temporaneo.
   - **Esempio:** Scansioni di rete frequenti da indirizzi IP noti per attività simili.
4. **Moderate Threat (3 teschi)**
   - **Descrizione:** Rappresenta un avversario capace con azioni dirette e determinate, spesso nella fase di consegna, sfruttamento o installazione.
   - **Esempio:** Documenti malevoli specificamente indirizzati a dipartimenti aziendali.
5. **High Threat (4 teschi)**
   - **Descrizione:** Attribuibile a un avversario avanzato, indicando attività mirata e persistente.
   - **Esempio:** Indirizzi di callback noti in log di accesso dopo un attacco mirato.
6. **Critical Threat (5 teschi)**
   - **Descrizione:** Avversario altamente qualificato e con risorse illimitate, critico in qualsiasi fase dell'intrusione.
   - **Esempio:** Attività di esfiltrazione dati in corso che richiede interventi immediati.

Confidence Rating (Valutazione di Fiducia)

Il Confidence Rating esprime quanto l'assessment del Threat Rating sia accurato, su una scala da 0 a 100:

1. **Confirmed (90–100)**
   - **Descrizione:** Valutazione confermata da fonti indipendenti o analisi diretta, coerente con altre informazioni.
   - **Esempio:** Un eseguibile noto per installare varianti di malware.
2. **Probable (70–89)**
   - **Descrizione:** Valutazione non direttamente confermata ma logica e coerente con altre informazioni.
   - **Esempio:** URL con path caratteristico di altri URL malevoli noti.
3. **Possible (50–69)**
   - **Descrizione:** Valutazione non confermata, logica ma solo parzialmente coerente con altre informazioni.
   - **Esempio:** Indirizzo email con username comune trovato in malware reverse-engineered.
4. **Doubtful (30–49)**
   - **Descrizione:** Valutazione possibile ma non la più logica, senza informazioni aggiuntive.
   - **Esempio:** Scansioni da un indirizzo IP di un provider VPS.
5. **Improbable (2–29)**
   - **Descrizione:** Valutazione possibile ma non logica, contraddetta da altre informazioni.
   - **Esempio:** Host di callback apparentemente inattivo.
6. **Discredited (1)**
   - **Descrizione:** Valutazione confermata come inaccurata.
   - **Esempio:** File non malevolo ma semplicemente mal formattato.
7. **Unassessed (0)**
   - **Descrizione:** Nessuna valutazione assegnata.
   - **Esempio:** Indicatori appena scoperti senza analisi iniziale.

Questi due livelli di valutazione aiutano a determinare l'importanza e l'urgenza con cui affrontare i vari indicatori di minaccia, fornendo un quadro chiaro per le decisioni operative all'interno delle organizzazioni (ThreatConnect Knowledge Base) (ThreatConnect Knowledge Base) (ThreatConnect Knowledge Base).

Traccia 2

1. **Prerequisiti**:
   - Assicurarsi di avere Python installato sulla tua macchina.
   - Installare i pacchetti necessari come `requests` se non li hai già.
   -
2. **Clonare il repository**:
   - Aprire il terminale e clonare il repository di TekDefense-Automater:

     ```
     bash
     git clone https://github.com/1aN0rmus/TekDefense-Automater.git
     ```

3. **Navigare nella directory del progetto**:

   ```
   bash
   cd TekDefense-Automater
   ```

4. **Installare le dipendenze**:
   - Installare le dipendenze richieste con:

     ```
     bash
     pip install -r requirements.txt
     ```

5. **Eseguire il software**:
   - Eseguire Automater con un bersaglio a scelta. Per esempio, se si volesse analizzare l'indirizzo IP `8.8.8.8` (un indirizzo IP pubblico di Google), utilizzare il comando:

     ```
     bash
     python automater.py -t 8.8.8.8
     ```

6. **Esempio di output atteso**:

   ```
   plaintext
   Host: 8.8.8.8
   Country: United States
   City: Mountain View
   Latitude: 37.386
   Longitude: -122.0838
   ```

7. **Interpretare i risultati**:
   - L'output fornirà varie informazioni sull'indirizzo IP o l'URL che si è scelto, incluse informazioni geografiche, e potenzialmente indicatori di minaccia associati al bersaglio.

Note Importanti

- **Autorizzazione**: Assicurarsi di avere l'autorizzazione per analizzare gli indirizzi IP o URL che stai utilizzando per evitare qualsiasi violazione legale.
- **Fonti di dati**: Automater utilizza vari servizi online per raccogliere informazioni. La disponibilità e l'accuratezza dei dati possono variare in base ai servizi utilizzati.